In re Patent Application of
ROMAIN
Serial No. 09/914,172
Filed: AUGUST 24, 2001

REMARKS

Applicant appreciates the Examiner's careful and thorough examination of the present application. Claims 7, 9-12, 14-17 and 19-22 remain pending in the application. Favorable reconsideration is respectfully requested.

I. The Claims

As described in the specification, security is provided in a chaining of operations performed by an electronic circuit by the presence of parasitic information which interferes with the observation, from the outside of the electronic circuit, of physical phenomena associated with the execution of useful operations. The invention provides invisibility regarding analysis of electrical signals related to data transfers between various registers.

Claim 7 is directed to a method for providing security to a chaining of useful operations, of a same type, performed by an electronic circuit executing an algorithm, each of the useful operations corresponding to a step of the algorithm. The method includes randomly introducing at least one dummy operation of the same type in the chaining of useful operations, and maintaining a constant time interval between execution of two successive useful operations.

Claim 12 is directed to a method for providing security to an electronic circuit executing an algorithm. The method includes executing the algorithm so that useful operations of a same type are chained together, with each useful operation corresponding to a step of the algorithm.

Again, the method includes maintaining a constant time interval between execution of two successive useful operations, and randomly introducing at least one dummy operation of the same type in the chaining of useful operations.

Claim 17 is directed to an electronic device including a processor for executing an algorithm that includes a plurality of useful operations of a same type, and a routine for providing security to a chaining of the plurality of useful operations, with each useful operation corresponding to a step of the algorithm. The routine randomly introduces at least one dummy operation of the same type in the chaining of useful operations, and the routine maintains a constant time interval between execution of two successive useful operations.

II. The Claims are Patentable

The Obviousness-type Double Patenting Rejection

Claims 7, 9-12, 14-17 and 19-22 were rejected on the grounds of obviousness-type double patenting as being unpatentable over claims 15, 16, 19 and 20 of U.S. Patent No. 6,971,020 (Liardet et al.) in view of U.S. Patent No. 5,944,833 (Ugon).

As the Examiner is aware, any obviousness-type double patenting rejection should make clear: (A) The differences between the inventions defined by the conflicting claims - a claim in the patent compared to a claim in the

application; and (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue would have been an obvious variation of the invention defined in a claim in the patent.

On pages 2 and 3 of the Office Action, the Examiner provides a comparison between the rejected claims of the present application and the issued claims of the patent, and asserts, that "Claims 7, 12 and 17 teach the similar limitations of claims 15-16 and 19-20 except 'maintaining a constant time interval between executive [sic] of two successive useful operations'." The Examiner further asserts that "Ugon discloses that start and end times of each instruction is [sic] can be known and observe by the clock signals of the program execution (see col. 1, lines 20-50)" and that it would then have been obvious to modify the patented claims in view of the Ugon teaching to arrive at the claimed invention.

The Examiner did not completely address the differences between the inventions defined by the allegedly conflicting claims. For example, Claim 15 of the patent is directed to a method for securing a cryptography coprocessor comprising: transmitting data by a first two-way link from a memory module to a battery of input/output registers, the battery of input/output registers comprising a scrambling register; transmitting data corresponding to a message to be processed by an encryption or decryption operation, through a multiplexer, from the battery of input/output registers to an input register; and transmitting digital key data for the

encryption or decryption operation comprising an unencrypted digital key and a plurality of scrambling bits intermixed with the digital key, through the multiplexer, from the battery of input/output registers to a key register while substantially simultaneously transferring the scrambling bits between the multiplexer and the scrambling register via a second, dedicated two-way communication link, and storing the scrambling bits, which are foreign to the message to be processed and the unencrypted digital key, in the scrambling register of the battery of input/output registers; using a processing module to determine the unencrypted digital key based upon the digital key data stored in the key register and the scrambling bits stored in the scrambling register; and performing the encryption or description operation on the message to be processed stored in the input register with the processing module based upon the determined digital key, and outputting the result of the encryption or decryption operation to an output register.

However, Claim 7 of the application is directed to a method for providing security to a chaining of useful operations, of a same type, performed by an electronic circuit executing an algorithm, each of the useful operations corresponding to a step of the algorithm. The method includes randomly introducing at least one dummy operation of the same type in the chaining of useful operations. The method of Claim 12 includes executing the algorithm so that useful operations of a same type are chained together, with each useful operation corresponding to a step of the algorithm. Again, the

method includes randomly introducing at least one dummy operation of the same type in the chaining of useful operations. Claim 17 is directed to an electronic device including a processor for executing an algorithm that includes a plurality of useful operations of a same type, and a routine for providing security to a chaining of the plurality of useful operations, with each useful operation corresponding to a step of the algorithm. The routine randomly introduces at least one dummy operation of the same type in the chaining of useful operations.

In a review of just these few examples, it is clear that the Examiner did not address nearly any of the differences between Claims 7, 12 and 17 of the application and the claims of the patent.

Accordingly, based upon at least the examples provided above, it should be clear that the Examiner has not clearly set forth the differences between the inventions defined by the conflicting claims or why such differences would have been an obvious as required in an obviousness-type double patenting rejection. For these reasons alone, the double patenting rejection is improper and should be withdrawn.

Additionally, since the analysis used in an obviousness-type double patenting rejection parallels the guidelines for analysis of a 35 U.S.C. §103 obviousness determination, Applicants will address the "obviousness" aspect of the double patenting rejection below.

In re Patent Application of
ROMAIN
Serial No. 09/914,172
Filed: AUGUST 24, 2001

The Ugon invention relates to an integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means for decorrelating the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit. The internal or external electrical signals include timing, synchronization and status signals.

The Examiner has misinterpreted the cited reference to Ugon. Specifically, the Examiner asserts (page 2-4 of the Office Action) that Ugon teaches that "start and end times of each instruction can be known and observed by the clock signals" and that this teaching somehow would render it obvious to maintain a constant time interval between execution of two successive useful operations to obscure the operation from being observed. The Examiner's assertion is puzzling because knowing the start and end times has nothing to do with whether a constant or variable time interval is used by the process. Indeed, there is no teaching of "maintaining a constant time interval between execution of two successive useful operations", as claimed.

Accordingly, even if it were obvious to modify the claims of Liardet et al. with the teachings of Ugon, the combination would still not meet the features of the claimed invention. Furthermore, it is clear that the Examiner is impermissibly using the teachings of Applicant's own patent application as a roadmap to modify the prior art. For example, in both the current and previous Office Actions (e.g. page 5),

the Examiner acknowledges that neither Ugon nor Cohen teach the use of a constant time interval as claimed.

For these additional reasons, the obviousness-type double patenting rejection is improper and should be withdrawn.

The Prior Art Rejection

Claims 7, 9-12, 14-17 and 19-22 were rejected in view of Ugon (U.S. Patent No. 5,944,833) in view of Cohen ("Operating System Protection Through Program Evolution") or further in view of Griffin et al. (EP0448262 or corresponding document U.S. Patent No. 5,249,294) for the reasons set forth on pages 3-6 of the Office Action. Applicant contends that Claims 7, 9-12, 14-17 and 19-22 clearly define over the cited references, and in view of the following remarks, favorable reconsideration of the rejections under 35 U.S.C. §103 is requested.

Each of the independent Claims 7, 12 and 17 at least includes randomly introducing at least one dummy operation of the same type in the chaining of useful operations, and the routine maintaining a constant time interval between execution of two successive useful operations. It is these combinations of features which are not fairly taught or suggested in the cited references and which patentably define over the cited references.

The Ugon invention relates to an integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means for

decorrelating the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit. The internal or external electrical signals include timing, synchronization and status signals.

The Cohen reference is concerned with the use of program evolution as a technique for defending against automated attacks on operating systems. The Examiner pointed to the section on "Garbage Insertion" for the teaching that any sequence of instructions that are independent of the in-line sequence can be inserted into the sequence without altering the effective program execution. Each added instruction increases both time and space, but can fool programs that look for specific instruction sequences. The technical field of Cohen is different from the field of the invention as Cohen relates to the protection against the modification of a program by another program, and the invention relates to the protection against the reading of confidential data.

The Griffin patent is concerned with determination of time of execution of a data processing routing in relation to an occurrence of a prior externally observable event. A procedure known as a "clock attack" is prevented by a method that inhibits synchronization with externally generated instructions by preventing determination of the time of execution predetermined data processing routine in relation to occurrence of an externally observable event that precedes the execution of the predetermined routine. The method includes the step of randomly varying the duration between the

occurrence of the externally observable event and the execution of the predetermined routine. The method also provides a delay of a variable duration between routines.

The operations in Griffin (interim routine) are implemented with operations (useful routine) which are not of the same type. Accordingly, Griffin does not suggest the insertion of a dummy operation of the same type in the chaining of useful operations.

The Examiner has misinterpreted the cited reference to Ugon. Specifically, the Examiner asserts (page 2-4 of the Office Action) that Ugon teaches that "start and end times of each instruction can be known and observed by the clock signals" and that this teaching somehow would render it obvious to maintain a constant time interval between execution of two successive useful operations to obscure the operation from being observed. However, Applicants point out that knowing the start and end times has nothing to do with whether a constant or variable time interval is used by the process. Indeed, there is no teaching of "maintaining a constant time interval between execution of two successive useful operations", as claimed. For this reason alone, the combination of teachings cannot result in the invention as claimed.

Furthermore, the Examiner is again impermissibly using the teachings of Applicant's own patent application as a roadmap to modify the prior art. Indeed, in both the current and previous Office Actions (e.g. page 5), the Examiner

acknowledges that neither Ugon nor Cohen teach the use of a constant time interval as claimed.

As the Examiner is aware, to establish a prima facie case of obviousness, there must be some suggestion or motivation, either in the reference itself or in the knowledge generally available to one of ordinary skill in the art, to modify the reference; and, the prior art reference must teach or suggest all the claim features. The initial burden is on the Examiner to provide some suggestion of the desirability of doing what the Applicants have done. To support the conclusion that the claimed invention is directed to obvious subject matter, either the reference must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the reference. Both the suggestion to make the claimed combination and the reasonable expectation of success must be founded in the prior art and not in Applicants' disclosure.

There is simply no teaching or suggestion in the cited references to provide the combination of features as claimed. Accordingly, for at least the reasons given above, Applicant maintains that the cited references do not disclose or fairly suggest the invention as set forth in Claims 7, 12 and 17. Furthermore, no proper modification of the teachings of these references could result in the invention as claimed. Thus, the rejections under 35 U.S.C. §103(a) should be withdrawn.

In re Patent Application of
ROMAIN
Serial No. **09/914,172**
Filed: **AUGUST 24, 2001**

It is submitted that the independent claims are patentable over the prior art. In view of the patentability of the independent claims, it is submitted that their dependent claims, which recite yet further distinguishing features are also patentable over the cited references for at least the reasons set forth above. Accordingly, these dependent claims require no further discussion herein.

III. Conclusion

In view of the foregoing remarks, it is respectfully submitted that the present application is in condition for allowance. An early notice thereof is earnestly solicited. If, after reviewing this Response, there are any remaining informalities which need to be resolved before the application can be passed to issue, the Examiner is invited and respectfully requested to contact the undersigned by telephone to resolve such informalities.

Respectfully submitted,

PAUL J. DITMYER
Reg. No. 40,455
Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
407-841-2343 fax
Attorney for Applicant

In re Patent Application of
ROMAIN
Serial No. **09/914,172**
Filed: **AUGUST 24, 2001**

CERTIFICATE OF FACSIMILE TRANSMISSION

I HEREBY CERTIFY that the foregoing correspondence has been forwarded via facsimile number 571-273-8300 to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 this 4th day of August, 2006.